WHAT IS CLAIMED IS:

1. A policy file for controlling cryptographic functions of an application program, comprising:

an attribute portion that holds a plurality of cryptographic policy attributes, each cryptographic policy attribute representing a cryptographic function;

a value portion that includes a plurality of attribute values, each attribute value corresponding to a separate one of the cryptographic policy attributes and indicating to a policy filter whether an application program may employ the cryptographic policy represented by the attribute; and

a signature portion for verifying authenticity of said attribute portion and said value portion.

2. The policy file of claim 1 wherein said plurality of cryptographic policy attributes includes cryptographic capabilities of said application program in a country where said application program is to be executed.

3. The policy file of claim 1 wherein each of said attribute values is a data string, an integer number, or a truth expression, said truth expression including one of a true flag, a false flag, or a conditional flag.

4. The policy file of claim 1 wherein said signature portion includes a digital signature and a chain of certificates, wherein said digital signature includes a certificate indicative of the origin of said digital signature and further, wherein said chain of certificates is indicative of the validity of said digital signature.

5. A system for controlling cryptographic functions of an application program, comprising:

storage means for storing a policy file, said policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stored a plurality of attribute values, and a signature portion, each of said attribute values corresponding to each of said cryptographic policy attributes, said signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from said policy file; and

processing means for selectively processing said retrieved encryption and/or decryption information from said policy file in accordance with a predetermined capability conditions, and for providing allowable encryption and/or decryption levels to said application program.

6. The system of claim 5 wherein each of said cryptographic policy attributes includes an indication of the cryptographic capabilities of said application program, and each of said attribute values is one of a string, an integer number, or a truth expression, and wherein said signature portion includes digital certificates for validating a signer's certificate.

7. The system of claim 6 wherein said truth expression is one of a true flag, a false flag, or a conditional flag.

8. The system of claim 5 wherein said storage means is an archive file.

9. The system of claim 5 where said plurality of attributes and values are compressed in said storage means, and further including decompressing means for decompressing said compressed plurality of attributes and values in accordance to said control means retrieving said compressed plurality of attributes and values.

10. A system for controlling cryptographic functions of an application program, comprising:

storage means for storing a policy file, said policy file including an attribute portion that stores a plurality of cryptographic policy attributes, a value portion that stored a plurality of attribute values, and a signature portion, each of said attribute values corresponding to each of said cryptographic policy attributes, each of said cryptographic policy attributes including an indication of the cryptographic capabilities of said application program, and each of said attribute values is one of a string, an integer number, or a truth expression, and said signature portion including digital certificates for validating a signer's certificate;

control means for selectively retrieving encryption and/or decryption information from said policy file; and

processing means for selectively processing said retrieved encryption and/or decryption information from said policy file in accordance with a predetermined capability conditions, and for providing allowable encryption and/or decryption levels to said application program.

11. The system of claim 10 wherein said storage means is an archive file.

12. The system of claim 10 where said plurality of attributes and values are compressed in said storage means, and further including decompressing means for decompressing said compressed plurality of attributes and values in accordance to said control means retrieving said compressed plurality of attributes and values.

13. A method of validating a cryptographic policy file for controlling cryptographic functions in an application program, said method comprising the steps of:

retrieving a policy file including an attribute portion, a value portion and a signature portion from a storage means;

verifying a digital signature on an attribute-value pair stored in said storage means;

performing a verification of said application program version with a software-version attribute value of said policy file in said storage means; and

confirming localization information of said application program with a localization in said software-version attribute value of said policy file.

14. The method of claim 13 wherein said policy file is determined invalid and ignored by said application program when any one of said verifying, performing and said confirming step fails.

15. The method of claim 13 further including the step of configuring each of said application cryptographic capabilities in accordance with said plurality of attribute-value pairs.

16. The method of claim 13 wherein said step of verifying includes determining that one or a plurality of the certificates in said digital signature certificate chain includes a certificate issued by a manufacturer of said application.

17. The method of claim 16 wherein said step of determining includes comparing said digital signature to a predetermined certificate.

18. The method of claim 17 wherein said predetermined certificate includes a certification authority (CA) certificate.